

STATE OF MONTANA

Montana Information Security Advisory Council
Best Practices Workgroup – Personnel Security

Personnel Security Standards



STATE OF MONTANA

Montana Information Security Advisory Council
Best Practices Workgroup – Personnel Security

1. Purpose

To further increase the overall security posture of the State of Montana, several agencies agreed to collaborate on a strategic goal of increasing security through efforts associated with Personnel Security. The category of Personnel Security as defined by NIST includes position risk designation, personnel screening, personnel termination, personnel transfers, access agreements, third-party personnel security, and personnel sanctions. This document has been concurred upon by the MT-ISAC membership, and approved as an enterprise standard by the Chief Information Officer for the State of Montana.

2. Policy

Personnel Security applies to the following controls found within the Information Security Policy.

a. [Information Security Policy](#)

- Identify
 - 2.4.11, 2.9.5.4, 2.9.5.5, 2.9.5.6, 2.14.12.1, 2.14.12.3, 2.14.12.4, 2.14.12.5, 2.14.12.6, and 2.15.8.
- Protect
- Detect
- Respond
- Recover

b. [Information Security Policy – Appendix A](#)

- Personnel Security (MP), pages 17- 20
 - PS-1 – Personnel Security Policy and Procedures
 - PS-2 – Position Risk Designation
 - PS-3 – Personnel Screening
 - PS-4 – Personnel Termination
 - PS-5 – Personnel Transfer
 - PS-6 – Access Agreements
 - PS-7 – Third-Party Personnel Security
 - PS-8 – Personnel Sanctions

3. Definitions of Personnel Security

Risk Designation is a measurement of the duties and responsibilities for a position and the degree of potential damage to the efficiency or integrity of the systems/services from misconduct of individual(s) in a position.

4. Personnel Security Best-Practices (PS 2 through PS-7)

STATE OF MONTANA

Montana Information Security Advisory Council
Best Practices Workgroup – Personnel Security

Risk Designations

In accordance with [MCA 2-15-114](#) (each department head is responsible for ensuring an adequate level of security of all data within that department) each agency shall:

1. Assign a risk designation to all positions;
 - a. Review and revise position risk designations every two years.

Personnel Screening

Based upon risk designations agencies shall:

1. Establish screening criteria to determine the suitability for the individuals filling those positions. Examples of screening criteria include, but are not limited to:
 - a. The type of background check required for the position
 - b. Classification of the data accessed by the position
 - c. Citizenship/residency
2. Perform risk based analysis to determine an appropriate level for background investigations should be conducted
3. Identify and apply additional screening requirements for those positions contained within Montana Code and other regulatory guidelines
 - a. See example:
http://www.leg.mt.gov/bills/mca/title_0050/chapter_0130/part_0030/section_0050/0050-0130-0030-0050.html
4. Screen individuals prior to authorizing access to information systems,
5. Rescreen individuals according to the following conditions: job-transfer/hire into a position that requires additional security access to raised floor areas or positions that are housed at secured data center facilities; as required by state policy (every 3 years). Refer to agency policy for internal transfers; and
6. Document any exceptions to the personnel screening standard.

Personnel Termination

The State of Montana, upon termination of individual employment:

1. Terminates all information system access;
2. Conducts exit interviews;
3. Retrieves all security-related organizational information system-related property; and
4. Retains access to organizational information and information systems formerly controlled by terminated individual

Personnel Transfer

STATE OF MONTANA

Montana Information Security Advisory Council
Best Practices Workgroup – Personnel Security

When reassigning or transferring personnel to other positions within the State, a review of logical and physical access authorizations to information systems/facilities is performed within three business days of beginning the new position to ensure access is limited to authorized and required systems/facilities.

See the following for FBI's background process:

<https://www.fbi.gov/services/cjis/identity-history-summary-checks>

5. Compliance

Compliance shall be evidenced by the implementation of the Personnel Security standards and the related best practices as described above.

6. Conclusion

The Personnel Security Standard document is the result of a multi-agency collaboration and has the MT-ISAC Best Practices Work Group approval. The representatives from these groups worked to endorse the recommendations contained here-in. A methodical, well-planned approach to effectively testing and measuring these controls will introduce additional layers to the security of the State of Montana's end-users.